REMARKS

In response to the Office Action dated February 21, 2008 ("the Office Action"), entry of the foregoing request for reconsideration regarding the above-identified application is respectfully requested in view of the following remarks.

I. Status of the Claims:

Claims 1-52 were pending in the application prior to submission of the current response. All of the claims have been rejected by the Examiner in the Office Action.

No claims have been amended in this response.

II. Rejections under 35 U.S.C. §103(a):

Claims 1-52 have been rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,236,596 to Francine J. Prokoski (hereafter "Prokoski") in view of U.S. Patent No. 7,003,113 to Kazuhiro Yanase (hereafter "Yanase") and further in view of U.S. Patent No. 5,799,083 to Brothers *et al.* (hereafter "Brothers").

A. Independent Claims:

Claim 1 recites:

> A method, comprising:
> determining a current location for a multimedia device using positional information provided by a long range cellular network or short-range wireless communication medium;
> computing location-based authentication data using the positional information;
> encoding multimedia content created on the multimedia device with said location-based authentication data by computing a hash value on a combined expression of the multimedia content, said location-based authentication data and identification data including at least one of user identification data and device identification data, wherein said encoding creates a content identity key that authenticates the multimedia content as being created at a certain physical location and time
> transmitting the encoded multimedia content to a content certification entity via wireless communication, the content certification entity verifying the authenticity of the encoded multimedia content based on the content identity key prior to distribution.

Prokosky discloses a digital video camera comprising an Imaging and Encoding Subsystem that includes a digital imaging sensor, a GPS receiver, a Greenwich Mean Time (GMT) receiver, the camera ID, a frame counter and an encoding generator. The camera captures and stores frames of imagery in a digital buffer, whereby the frame number is incremented and stored. The GMT receiver captures and stores the time; and GPS receiver captures and stores the location. FIG. 1 shows a method of encoding imagery captured by the camera. Namely, the image is captured, and then authentication information is recorded at the time and place of capturing. An encoding process uses the camera ID, frame location, and time to produce an encoded image. An encrypter encrypts the encoded image to produce an encrypted encoded image (step 109 in FIG 1). The resultant image is transmitted, output or stored (step 112). [C6, L60 – C7, L17].

The Office Action sets forth that Prokosky "does not explicitly disclose the certification authority receiving the encoding content for authentication." [Office Action, page 3—lines 1-3]. In addition, Applicant respectfully notes that Prokosky does not teach or suggest "transmitting the encoded multimedia content to a content certification entity via wireless communication." In an attempt to remedy Prokosky's deficiency with regard to the above-described feature, the Office Action provides that "Brothers disclosed the trusted third party being used for authentication see Col 8 Ln 53-56." [Office Action, page 3—lines 7-8].

Brothers is directed to an event verification system 10, as shown in FIG 1, which comprises a trusted third party 12 and a video camera 14 which employs a single key encryption technique. The trusted third party 12 creates a secret key using a key generator 16 and programs the camera with the secret key and an authentication code that is unique to the key. [C3, L33-41]. FIG. 3 of Brothers illustrates another event verification system 48 comprising a trusted third party 12 and a video camera 14 which employs a public key encryption technique. The trusted third party 12 creates a public/private key pair and programs the camera with the public/private key pair and an identification code unique to the public/private key pair. [C5, L61 – C6, L5]. In other words, as disclosed by Brothers, the key and its related unique code are used for programming and authentication of camera 14. See e.g., C6, L42-57: "[w]hen the camera 14 is brought to the trusted third party 12 for key programming, the trusted third party 12 uses a security verification unit 54 to perform an electronic handshaking routine… In the event that the

tamperproof enclosure 20 has been breached or compromised, the electronic handshaking will fail, and the trusted third party 12 will not program the camera 14." Moreover, Brothers discloses that "[i]f authentication of a recorded event is required, the verification process can be performed by any party obtaining the public key from trusted third party 12." This means that other entities "with an interest in the authenticity of the recorded events can verify the authenticity of an electronic recording without having to further employ the services [of] the trusted third party 12." [See C8, L17-42].

Applicant respectfully submits that Brothers does not teach or suggest "the certification authority receiving the encoding content for authentication," and therefore, disagrees with the Examiner's assertions in the Office Action. Moreover, Brothers also does not teach or suggest "transmitting the encoded multimedia content to a content certification entity", as recited in claim 1. Brothers only discloses that the trusted party 12 creates a secret key and programs the camera with the secret key and an authentication code, for purposes of authenticating the camera. In contrast, claim 1 recites "the content certification entity verifying the authenticity of the decoded multimedia content based on the content identity key prior to distribution." Contrary to claim 1 (e.g., authenticating multimedia content "prior to distribution"), Brothers requires users "with interest in the authenticity of recorded events" to obtain their own sources for "verifying the authenticity of an electronic recording without having to employ the services [of] the trusted third party 12." As a result, Brothers in actuality teaches away from "the content certification entity **verifying the authenticity of the encoded multimedia content** based on the content identity key **prior to distribution**" as recited in claim 1.

In addition to the forgoing, the Office Action concedes that "neither Prokosky nor Brothers disclose the using of positional information for authentication." In particular, Applicant respectfully notes that neither Prokosky nor Brothers disclose "using positional information provided by a long range **cellular network** or a short-range wireless communication medium," as recited in claim 1. Nevertheless, in an attempt to fulfill the lack of teaching of the above-named features in Prokosky and Brothers, the Office Action asserts that "Yanase discloses the positional information being used for authentication see Col 2 Ln 36-45." Applicant respectfully disagrees.

Yanase is drawn to a position authentication system and electronic equipment using the same. FIG. 1 of Yanase illustrates a digital camera 1 with a GPS receiver 2 and storage device 3. The digital camera 1 writes photographed image data into the storage device 3, and at the same time, it receives GPS electric wave 5 from GPS receiver 2 and generates latitude/longitude information. The GPS receiver 2 encrypts and transmits the latitude/longitude information as position information to center system 4. The center system 4 uses the position information to generate place-specifying data to apply to a copy guard process and transmits the place-specifying data to the digital camera 1. [C3, L60 – C4, L24]. Accordingly, Yanase discloses using position information to generate place-specifying data to apply to a copy guard process.

In view of the above, Applicant respectfully asserts that Yanase does not teach or suggest "positional information provided by a long range cellular network or a short-range wireless communication medium", or "computing location-based **authentication data** using the positional information". Moreover, Yanase does not resolve the deficiencies noted above in reference to Brothers and Prokosky. Namely, Yanase does not disclose or suggest "transmitting the encoded multimedia content to a content certification entity via wireless communication, the content certification entity verifying the authenticity of the encoded multimedia content based on the content identity key prior to distribution," as recited in claim 1.

As a result, Applicant respectfully contends that none of the cited references (i.e., Prokosky, Brothers and Yanase), either taken alone or in combination, teach or suggest at least "transmitting the encoded multimedia content to a content certification entity via wireless communication, the content certification entity verifying the authenticity of the encoded multimedia content based on the content identity key prior to distribution", as recited in claim 1. Accordingly, claim 1 is believed to be patentably distinguished from the cited references. Independent claims 14 and 52 include at least the distinguishable features discussed above with respect to claim 1. Therefore, Applicant respectfully asserts that independent claims 1, 14 and 52, and claims dependent thereupon, are allowable over the cited references.

Further to the forgoing arguments regarding the allowability of claim 1, Applicant respectfully notes that claim 26 recites additional features that are neither taught nor suggested

by the cited references. Namely, in addition to features similar to those found in claim 1, claim 26 recites, *inter alia:*

> receiving digital multimedia content created on a multimedia device into a context server through a wireless communication network;
> receiving location-based authentication data computed using the positional information through a network into an authentication server, wherein the location-based authentication data is correlated with the multimedia device that created the multimedia content;
> forwarding the correlated location-based authentication data to the context server; and
> executing an encryption algorithm in the context server, wherein the correlated location-based authentication data is encoded into the multimedia content by computing a hash value on a combined expression of the multimedia content said location-based authentication data and identification data including at least one of user identification data and device identification data, to create a multimedia content identity key that authenticates the multimedia content as being created at a certain physical location and time.

In accordance with at least one exemplary embodiment, there exists an interaction between a context server and an authentication server, wherein the context server may receive multimedia content and the authentication server may separately receive location-based authentication which is then correlated. The correlated location-based authentication information may then be passed to the context server where it is encoded into the multimedia content.

Regarding claim 26, the Office Action concedes that Prokosky "dos not explicitly disclose the context server receiving the encoding content for authentication." Nevertheless, the Office Action asserts that "Brothers discloses the trusted third party being used for authentication see Col 8 Ln 53-56." However, even after modifying Prokosky with Brothers, the Office Action further concedes that "neither Prokoski nor Brothers disclose the using of positional information for authentication." In an attempt to remedy the lack of teaching of the above-named features in Prokosky and Brothers, the Office Action provides that "Yanase discloses the positional information being used for authentication into an authentication server (i.e. central system) see Col 2 Ln 36-45 & Fig. 1 item 4."

As discussed above, Brothers only discloses that the trusted party 12 creates a secret key and programs a camera with the secret key and an authentication code, for purposes of authenticating the camera, whereby users that require authentication of media content (e.g. an electronic recording) must do so without employing the services of the trusted third party. [See

e.g. Brothers C8, L17-41]. In contrast, claim 26 recites "the content certification entity **verifying the authenticity of the decoded multimedia content** based on the content identity key **prior to distribution**." The teachings of Prokosky and Yanase have been thoroughly discussed above in connection with claim 1. Applicant respectfully asserts that the combination of references, as proposed by the Office Action, do not teach or suggest "a context server" and "an authentication server" in the context required by claim 26.

As a result, Applicant respectfully submits that the cited references, either taken alone or in combination, do not render obvious claim 26. Independent claim 39 includes at least similar features as those found in claim 26. Accordingly, claims 26 and 39, and claims dependent thereupon, are also patentably distinguishable from the cited references.

II. Dependent Claims:

Claim 4 recites, *inter alia,* "the physical location is determined through a connection to a personal area network."

Claim 5 recites, *inter alia*, "the physical location is determined through a connection to a Bluetooth™ terminal."

Claim 6 recites, *inter alia*, "the physical location is determined through a connection to a WLAN terminal."

Regarding claims 4-7, the Office Action provides "Yanase discloses the different types of networks see Col 5 Ln 33-49." Column 5, lines 33-49 of Yanase read as follows:

> In FIG. **4**, a user takes a photograph of a desired subject by using digital camera **15** to obtain image data, and the image data thus obtained are written into processor **16** of the digital camera **15**. At the same time, GPS receiver **2** receives GPS electric wave **5** transmitted from GPS satellite group **8** at all times to generate latitude/longitude information, and inputs the latitude/longitude information to the processor **16**.
>
> The processor **16** encrypts the image data and the latitude/longitude information corresponding to the image data on the basis of a predetermined encrypting key, and transmits these data to center system **20**. The center system **20** receives transmission information from the digital camera **15**, and decodes the information by authentication unit **21** thereof. If the decoding is carried out normally, decoded image data **23** are supplied to copy guard device **22**, and also supplies latitude/longitude information **12** to place specifying data base **10**.

Applicant respectfully submits that Yanase does not teach or suggest any of the recited features of the above-listed claims 4-7. Applicant has also carefully reviewed the remainder of the Yanase, Prokosky and Brothers disclosures and finds no teachings of the features recited in claims 4-7. Thus, for at least this reason, the cited references, taken alone or in combination, do not render obvious claims 4-7.

Applicant does not believe it necessary at this time to further address the rejections of other dependent claims as Applicant believes that the forgoing amendments and remarks patentably distinguish all of the pending claims over the cited references. Applicant, however, reserves the right to address those rejections in the future should such a response be deemed necessary and appropriate.

* * *

In view of the foregoing, Applicant respectfully asserts that all of the presently pending claims, in the present form, are patentably distinguishable over Prokosky, Brothers and Yanase, either taken alone or in combination, and the rejections thereupon should be reconsidered.

CONCLUSION

Based on the foregoing amendments and remarks, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims and allowance of this application.

AUTHORIZATION

The Commissioner is hereby authorized to charge any additional fees which may be required for consideration of this Amendment to Deposit Account No. **13-4500**, Order No. 4208-4038. A DUPLICATE OF THIS DOCUMENT IS ATTACHED.

In the event that an extension of time is required, or which may be required in addition to that requested in a petition for an extension of time, the Commissioner is requested to grant a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to Deposit Account No. **13-4500**, Order No. 4208-4038. A DUPLICATE OF THIS DOCUMENT IS ATTACHED.

Respectfully submitted,
MORGAN & FINNEGAN, L.L.P

Dated: May 21, 2008

By: _____
Elliot F. Frank
Registration No. 56,641

Correspondence Address:
Address Associated With Customer Number:
27123

(212) 415-8700 Telephone
(212) 415-8701 Facsimile